



(07) 3847 8119
Level 1, 116 Ipswich Rd, Woolloongabba QLD 4102
PO Box 177, Coorparoo QLD 4151
fbaa.com.au

Australian Securities and Investments Commission

Strategy Group

Attn: Niki De Mel

Via email: BR.submissions@asic.gov.au

1st June 2021

The FBAA welcomes the opportunity to make a submission to ASIC's consultation under CP340: Breach reporting and related obligations.

Introductory Comments

1. We refer to our earlier submissions regarding breach reporting for credit licensees through which we have expressed some concerns over the complexity of the breach reporting obligations and the uncertainty that complexity causes. Our focus is to ensure the guidance provided to credit licensees is accurate, relevant and capable of being understood and implemented. Importantly, most of the more than 4,800 credit licensees in Australia are small to medium businesses having their first experience with a breach reporting regime.
2. It is important to acknowledge that real-time breach reporting requirements are a new concept to most credit licensees.
3. The FBAA has previously raised concerns with the approach of providing guidance to credit licensees by comparison/reference to the Corporations Act or financial services laws. Our preference is to see separate guidance for financial services and for consumer credit. It should not be necessary to expect credit licensees to have an understanding of the AFSL breach reporting regime in order to understand their breach reporting obligations under the NCCP Act.
4. The examples and case studies provided in the draft regulatory guide are taken from REP 594: *Review of selected financial services groups' compliance with the breach reporting obligation*¹. REP 594 could only include financial services firms as it was produced in 2018 and at a time where credit licensees were not under a similar breach reporting obligation. The 12 entities included in this review were many of the largest financial institutions in the country. The financial institutions included in the review likely account for the majority of employees, reps and fund flows in the country. Regulators need to remain mindful that the issues noted in REP594 and those also considered by the ASIC Enforcement Review Taskforce and Royal Commission which drove many of the breach reporting reforms (issues such as legalistic interpretations of the obligations, delays and failure to report breaches by juggernaut licensee groups) may not provide the right perspective to impose reporting obligations for the thousands of other licensees impacted by these rules. What works for a bank may not work for a single person or small licensee employing a handful of people and directly supervising their staff.
5. Our observation is that there could be more examples provided in Revised RG78 that are aimed at smaller licensees. They are the largest audience of the guidance by number. The types of issues that arise for smaller licensees include one-off breaches (as opposed to significant, systemic issues), acts or omissions of single representatives and procedural incidents arising from lack of awareness or oversight.

¹ RG78.9

Responses to consultation paper questions

Proposal	Your feedback
B1 We propose to give consistent guidance for AFS licensees and credit licensees on how they can comply with the breach reporting obligation, with examples of how the obligation applies in particular situations.	<p>B1Q1 Do you agree with our proposed approach? If not, why not?</p> <p>B1Q2 Are there differences in the structure or operation of credit licensees that require specific guidance on how the breach reporting obligation applies?</p>
<p>FBAA response:</p> <p>Our preferred option is to have separate guidance for financial services and for consumer credit since the regimes differ in as many ways as they share commonalities.</p> <p>We recognise there is no appetite to produce separate guidance for each regime in which case the next best outcome is to produce guidance that is as consistent as it can be for AFS and credit.</p> <p>QB1Q2 highlights to some extent the issue we have raised about referencing the obligations of credit licensees against the obligations that arise under the Corporations Act and Financial Services Laws. To answer the question about whether there are <i>differences</i> in the structure or operation of credit licensees we need to reference it back to the structure and operation of financial services licensees. We must know the AFS regime well enough to know how it <i>differs</i> from the credit regime.</p> <p>One of the notable attributes of the operation of credit licensees and the services they perform is the role of intermediaries. Intermediaries play a very significant role in the delivery of credit services. Intermediaries include aggregators, mortgage managers and referrers. We believe the RG needs content recognising the role that intermediaries play and the guidance should provide examples of situations where a breach or potential breach impacts multiple parties. The draft guidance already recognises that a party may not be required to report a breach in circumstances where another party may have already lodged a breach notification for the same issue although more clarity and reassurance could be provided. The potential penalties for not reporting a breach are significant. Many licensees would rather duplicate a breach report to ASIC rather than risk not reporting something where heavy penalties apply. It would be helpful for the guidance to provide as much clarity/reassurance as possible around what steps a licensee needs to take to demonstrate that it was reasonable to rely on another licensee lodging a breach report. Guidance may also help licensees understand which party should lodge a breach report where multiple parties are involved.</p>	
B2 We propose to include case studies and scenarios to supplement our general guidance and help illustrate key principles as they might apply to different licensees, industries and business models.	<p>B2Q1 Are there any specific issues, incidents, challenges or areas of concern you think we should include as examples, case studies or scenarios? If so, please provide details and explain why they should be included.</p>
<p>FBAA response:</p> <p>As referenced earlier, we recommend examples of situations that smaller licensees face on a regular basis. Examples could include: the failure to give out a particular document within the stipulated timeframe – or at all; issues with the conduct of representatives; loss of key staff; complaints.</p>	
B3 Draft RG 78 identifies where the existing breach reporting obligation (as in force immediately before 1 October 2021) continues to apply to AFS licensees: see draft RG 78.14–RG 78.18.	<p>B3Q1 Should we include further guidance to help AFS licensees understand how the existing breach reporting obligation under s912D of the Corporations Act (as in force before 1 October 2021 applies? If so, please provide details.</p>

FBAA response:
This section is not relevant in credit licensee guidance.

Proposal	Your feedback
<p>B4 We propose to provide high-level guidance to help AFS licensees and credit licensees identify what they must report to ASIC, including guidance on:</p> <p>(a) what is a 'reportable situation' (see draft RG 78.19–RG 78.25);</p> <p>(b) whether a breach or likely breach of a core obligation is significant (see draft RG 78.26–RG78.45);</p> <p>(c) when an investigation is a reportable situation (see draft RG 78.46–RG 78.57);</p> <p>(d) what are 'additional reportable situations' (see draft RG 78.58–RG 78.60); and</p> <p>(e) what are reportable situations about other licensees (see draft RG 78.61–RG 78.67).</p>	<p>B4Q1 Do you agree with our proposed approach? If not, why not?</p>
<p>FBAA response: Yes we support the high-level guidance approach. More specific comments against each area are made below.</p>	
<p>B4Q2 Should we include further guidance on what constitutes a 'core obligation'? If so, please provide details.</p>	
<p>FBAA response: We recommend considering moving paragraphs 78.21 and 78.22 down below the existing paragraph 78.27. The reason we say this is that para 78.21 introduces discussion around the concept of a 'core obligation' before it is defined at 78.29. This may send readers off looking for the definition of core obligation before they read further into the guide. 78.21 and 78.22 appear to be a better fit under the heading "What is a breach or a likely breach of your core obligations?" at 78.27. This is also where the Appendix is first referenced.</p> <p>We otherwise believe the definition of 'core obligation' is adequately explained at 78.29 (noting again that a credit licensee must read past the irrelevant guidance at 78.28 pertaining to AFS) and in the Appendix.</p>	
<p>B4Q3 Should we include further guidance on how to determine whether a breach or likely breach of a core obligation is 'significant'? If so, please provide details.</p>	
<p>FBAA response: We recommend reviewing the consumer credit insurance example at 2(a) in Table 2. We understand the desire to get such an example into the guidance. The current wording of the example does not make it clear how causing an individual consumer to pay \$153 in unsuitable premiums could be seen as "material loss or damage". It is not expected that a licensee would consider \$153 material to the point it would self-report a breach to ASIC. It is not correct to suggest an individual consumer who has paid \$153 has somehow lost more than that because others may have also paid a similar amount. The loss or damage to each consumer is confined to the individual amount they paid.</p>	

The wording should be clearer if ASIC believes that the significance test applies to the total collected by the insurer and believes it would be a material breach if the amount collected by the insurer were substantial. This would similarly apply to a large financial institution collecting a few dollars from millions of accounts. The total would be a material sum to the institution but a negligible amount to each customer.

In most cases it would be unreasonable to expect a licensee to measure the materiality of the sum of money against the demographic. There must still be a materiality threshold even if \$153 is a lot of money to a certain demographic. We think that by including this last sentence under the example it further confuses the message. It causes us to ask whether the breach is about \$153 being material to a student and therefore reportable (which it should never be) or is the materiality of the breach determined by the total collected by the insurer?

B4Q4 Should we include further guidance on reporting an 'investigation' to ASIC? If so, what should be clarified? Please provide examples of scenarios (where relevant).

FBAA response:

We have several concerns with Case Study 1.

1. It is not a good example for the issue. This is not a situation where an investigation and remedy would have been effected within 30 days, therefore it would have been significant and reportable. It should be clarified that Case study 1 (RG78.53) was still a reportable breach as the lender did not provide benefits to their customers and overcharged them. This appears to be a factual scenario that would fall under RG78.55
2. We do not understand the relevance of the issue being associated with home loan offset arrangements "within the broker channel". If a lender has an offset product and there is a defect in its systems that results in certain benefits and calculations being incorrectly applied then the defect would apply to all customers of that product. How is it relevant whether those customers were direct customers of the lender or came in through a broker channel? We circulated this Case Study to senior practitioners who agreed the reference to a lender product issue being attributed to the broker channel was confusing. Perhaps this Case Study has been concocted from a real example that ASIC has but if so it is an obscure issue and without the full understanding the background the Case Study does not make a lot of sense.
3. Case Study 1 reads more as though it is an attempt to try to make it relevant to brokers when it is clearly about a breach by a product issuer/lender and has nothing to do with brokers.

We do not support Case Study 1 as a fair or clear example of a typical scenario.

B4Q5 Should we include further guidance on what constitutes 'material loss or damage'? If so, what are the challenges licensees face in determining whether loss or damage is material? Please provide examples of how you consider questions of material loss or damage.

FBAA response:

We refer to our answer under B4Q3.

B4Q6 Should we include further guidance on reportable situations involving serious fraud or gross negligence? If so, what are the challenges licensees face in identifying when serious fraud or gross negligence has occurred?

FBAA response:

We do not see a need for further guidance on serious fraud or gross negligence.

B4Q7 Should we include further guidance on reportable situations about other licensees? If so, please provide details.

FBAA response:

Yes. Provide a credit-related example involving multiple parties. The ideal example is one involving a lender, an aggregator and a mortgage broker licensee/rep. All of industry wants greater clarity around ASIC's expectations about which parties need to report breaches to ASIC where there are multiple parties involved. The example could tie in the content of RG78.66 and address 2 scenarios – one where a licensee believes a breach report has already been lodged by another licensee and another example where it is not so clear. It would be possible to include these additional examples as variations to Table 7 Example 6(a). It would also be helpful to explain which party (if any) bears primary responsibility to report the breach or any guidance as to how the parties would determine which party lodges the breach report.

Proposal	Your Feedback
B5 We propose to include guidance in draft RG 78 about the obligation for licensees to report to ASIC within 30 days after they first know that, or are reckless with respect to whether, there are reasonable grounds to believe a reportable situation has arisen: see draft RG 78.68–RG 78.81.	<p>B5Q1 Should we include further guidance to help licensees understand when to report to ASIC? If so, please provide details, including what guidance would be helpful and why.</p> <p>B5Q2 Should we include further guidance on what may amount to 'knowledge', 'recklessness' and 'reasonable grounds'? If so, please explain what specific guidance would be helpful and why.</p> <p>B5Q3 Should we include any additional or alternative guidance to help licensees provide reports to ASIC in a timely manner? If so, please give details.</p>
<p>FBAA response:</p> <p>This section of the guidance appears clear.</p>	

Proposal	Your feedback
B6 We propose to provide general guidance on the types of information we will include in the prescribed form that licensees must use to provide reports to ASIC: see Table 8 in draft RG 78	<p>B6Q1 Do you have any feedback about the types of information we propose must be included in the prescribed form? If so, please provide details, and identify any issues.</p> <p>B6Q2 Should we include any other information in the prescribed form? If so, please provide details.</p> <p>B6Q3 Do you have any concerns about the types of information in the prescribed form and whether this information can be provided within the prescribed 30-day time period? If so, please provide details.</p>

FBAA response:

The guidance should reflect the fact that many licensees impacted by these new breach reporting obligations are not large financial institutions with compliance and legal departments. To that end it would be helpful to distinguish between information ASIC must have in a breach notification versus information it would be nice to have. It is detrimental to all parties if the notification form requires too much information or information of a type that licensees may not be able to produce without seeking external assistance. A licensee may be concerned that certain conduct or an omission should be reported as a breach and should be able to do so without having to identify the sections of the National Credit Act that are relevant. ASIC is better placed to identify the relevant provisions of the credit legislation or make a determination about the significance of the breach because they have a frame of reference set by breach reports being received from other licensees.

B7 We propose to provide high-level guidance on compliance systems for breach reporting to help licensees comply with the breach reporting obligation: see Section D of draft RG 78.

B7Q1 Do you agree with our proposed approach? If not, why not?
B7Q2 Are there any other specific areas that we should consider including in our guidance? If so, please provide details.
B7Q3 Are there any challenges that you would face in applying our guidance to your specific circumstances (i.e. the nature, scale or type of your business)? If so, please provide details.

FBAA response:

This section is technology neutral and recognises the scalability of the obligations relative to the size of the licensee. We make no further submission against this question.

C1 We propose to provide guidance for AFS licensees who are financial advisers and credit licensees who are mortgage brokers. The new obligations require these licensees to notify, investigate and remediate affected clients in certain circumstances. We have set out our proposed guidance in an information sheet: see draft INFO 000 in Attachment 2 to this paper.

C1Q1 Do you agree with our proposed approach? If not, why not?
C1Q2 Should the guidance we provide on the new obligations be provided in the form of a separate information sheet, or be incorporated into RG 256? Please provide details.
C1Q3 Should we include further or more specific guidance on the circumstances in which licensees must:
(a) notify affected clients of a breach of the law;
(b) investigate the full extent of that breach; or
(c) remediate affected clients?
If so, what other information would be helpful in determining how these obligations apply?

FBAA response:

Yes we agree with the approach. The information should be provided as a separate InfoSheet.

C2 We propose to give high-level guidance to AFS licensees and credit licensees about the types of information we consider should be included in the notices that must be given to affected clients: see in Actions 1 and 3 of draft INFO 000 in Attachment 2 to this paper.


C2Q1 Do you agree with our proposed approach? If not, why not?
C2Q2 Should the form of the notices referred to in Actions 1 and 3 of the information sheet be approved by ASIC? If so, what information, or types of information, should be mandatory, and what should be left to the discretion of the licensee?

FBAA response:

We agree with this approach. We would commence these new obligations from the position that it is not necessary for the form of notices to be approved by ASIC at this stage. A licensee will need to report the breach to ASIC and would presumably need to provide a copy of any communications sent to clients as part of their breach notification (or ASIC would subsequently request it). It would only be necessary to move towards an ASIC-approved form if the notifications being sent out by licensees are not adequate. ASIC could review this at a later stage. At this time give licensees the freedom to prepare their own notifications.

End.

Yours faithfully



Peter J White AM MAICD
Managing Director

Life Member FBAA
Life Member Order of Australia Association

Executive Chairman & Co Founder The Safety Space Foundation
Advisory Board Member Small Business Association of Australia (SBAA)
Chairman of the Global Board of Governors International Mortgage Brokers Federation (IMBF)